DOCUMENT OF THE INTER-AMERICAN DEVELOPMENT BANK
MULTILATERAL INVESTMENT FUND

CHILE

PROGRAM TO STRENGTHEN CHILEAN E-COMMERCE SECURITY AND TRUST

(TC-02-05-02-4-CH)

DONORS MEMORANDUM

This document was prepared by the project team consisting of: Gregorio Arévalo (RE1/FI1), Team Leader; Antonio Ca'Zorzi (SDS/ICT); Masami Yamamori (MIF); Patricio Díaz (COF/CCH); Alexandra Monteiro-Reed (LEG); Carlos Alberto Goldani (consultant, RE1/FI1); and Haydemar Cova (RE1/FI1).

CONTENTS

ANNEXES

ABBREVIATIONS

ABP	Alianza para las Buenas Prácticas en Internet [Alliance for Good Internet Practices]
ASP	Application Service Provider
ASR	Autorregulación, Sello de Confianza y Resolución de Conflictos [Self-regulation, seal of trust and conflict resolution]
BBB	Better Business Bureau
CAM	Centro de Arbitraje y Mediación [Arbitration and Mediation Center]
CCS	Cámara de Comercio de Santiago [Santiago Chamber of Commerce]
CED	Centro de Estudios de la Economía Digital [Center for Studies on the Digital Economy]
CORFO	Corporación de Fomento de la Producción [Chilean Economic Development Agency]
CPS	Certification Practices Statement
DE	Digital economy
ICT	Information and communication technology
MSMB	Microenterprise and small and medium-sized business
PCU	Program coordination unit
PKI	Public Key Infrastructure
PPMR	Project performance monitoring report
RA	Registration Authority
SICE	Seguridad Integral para el Comercio Electrónico [comprehensive security for e-commerce]
SME	Small and medium-sized enterprise

PROGRAM TO STRENGTHEN CHILEAN E-COMMERCE SECURITY AND TRUST

(TC-02-05-02-4-CH)

EXECUTIVE SUMMARY

Requester and executing agency:	Santiago Chamber of Commerce (CCS)	
Financing:	MIF (Facility I):	US$1,000,000
	Local counterpart:	US$1,000,000
	Total:	US$2,000,000
Execution timetable:	Execution period:	36 months
	Disbursement period:	42 months

Beneficiaries: The principal beneficiaries of the project will be the Chilean microenterprises and small and medium-sized businesses (MSMBs) that will have access to a secure and trustworthy system for carrying out business transactions via the Internet. This will permit these companies to explore and expand their markets using information and communication technology (ICT) tools to increase their competitiveness. Thanks to the comprehensive security for e-commerce (SICE) and the self-regulation, seal of trust and conflict resolution (ASR) components, consumers will have greater security for their electronic transactions, thus generating user confidence and stimulating growth in Internet-based transactions.

Objectives: The overall objective (end) of the program is to help improve the competitiveness of Chilean MSMBs. The specific objective (purpose) is to develop security services and applications and establish self-regulation mechanisms and the use of good Internet practices, thereby generating trust in the new information and Internet technologies, and encouraging their expanded and productive use throughout society.

Description: This operation is structured around two main components: (a) the component that deals with the **generation of confidence in the Internet environment: self-regulation – seal of trust – conflict resolution for e-commerce (ASR)** provides for the standardization and subsequent dissemination of policies and standards related to privacy and security, good business practices, and integrity of e-commerce transactions; and (b) the component that deals with **comprehensive security for e-commerce (SICE),** whose goal is to

provide cutting-edge e-business security solutions. This will help create an atmosphere of trust that will facilitate Internet-based electronic transactions and business operations through the provision of electronic security services to companies, and internationally recognized digital certificates issued locally. In addition, **dissemination** activities will be carried out and mechanisms implemented to **monitor and track** best e-commerce and security practices on a national and international level.

Special contractual clauses: The first disbursement of the financing will be subject to submission by the CCS of: (i) evidence of having set up the coordinating unit; (ii) an agreement establishing e-certchile's obligations vis-à-vis execution of component 2 of the program; and (iii) an annual execution plan for the first year, itemized by component (see paragraph 9.1).

Exceptions to Bank policy: None.

Environmental and social impact: The Committee on Environment and Social Impact reviewed the abstract for this operation at its meeting 35-02 held on 20 September 2002, and did not require any special evaluations or actions. The project team was advised to make an effort to ensure that indigenous companies also have access to the benefits of the program (see paragraph 3.8).

I. COUNTRY AND PROGRAM ELIGIBILITY

1.1 At its meeting of 6 October 1993, the Donors Committee declared Chile eligible for all of the financing modalities provided for under the Multilateral Investment Fund (MIF). The MIF declared this operation eligible under the Technical Cooperation Facility (I), inasmuch as it seeks to promote security and trust in the e-commerce market. The proposed project is part of the cluster of projects designed to strengthen the competitiveness of small and medium-sized enterprises (SMEs) through information and communications technology (ICT) (document MIF/GN-83). This cluster promotes the application and adoption of innovative ICT tools and solutions for SMEs in the region.

II. BACKGROUND

A. Information and communications technologies (ICT) and microenterprises and small and medium-sized businesses (MSMBs) in Chile

2.1 The rapid emergence of the Internet and the convergence of information and communication technologies have given rise to a new paradigm for technology and production, with the greatest demand coming from users in the developed countries. Seventy-five percent of Internet use originates in these countries, which generate 97% of e-commerce worldwide. Most of its benefits are thus concentrated in the most developed countries. The result is a process of cultural, economic and productive divergence among different groups of countries.[1]

2.2 In the case of Chile, sound models for applying the new technologies to business are emerging. This is the beginning of the process that will result in the widespread adoption of e-business techniques, until they become the standard. By the end of 2001, Chile was estimated to have 3,100,000 Internet users, representing 21% of the population and the highest penetration in Latin America. By 2004, Chile's Internet penetration is expected to reach 30% of the population, that is, almost 5 million users nationwide.

---

[1] Studies of some European countries found that ICT increased productivity between 0.3% (Germany) and 0.5% (France and Holland) for the 1996-1999 period. In the United States, 75% of productivity gains are estimated to have come from the use of ICT during that period. In the late 1990s, information technologies accounted for one quarter to one third of U.S. economic growth. In France, more than 20% of growth between 1996 and 1999 was estimated to derive from the use of ICT. This percentage falls to 17% for Germany, 16% in Italy and 13% in Holland. Chile still falls far below these levels, with estimates that ICT-related growth reached 7% in the same period.

2.3 According to estimates of the Santiago Chamber of Commerce (CCS), Chile's digital economy (DE)[2] exceeded US$5.7 billion in 2001, or more than 8% of gross domestic product. This represented an increase of 37% over the previous year. E-commerce could come to represent more than 50% of the digital economy in 2004, with an average annual growth rate of nearly 40% over the next few years. Much of that growth is likely to be in business-to-business (B2B) electronic transactions. This rapid growth in the digital economy reaffirms that the use of ICT in productive activities is increasing as it is adopted by a growing number of companies, resulting in a less visible but more functional Internet that can add greater value to people and businesses.[3] Some recent events, such as the enactment of the Digital Signature Law, are helping to facilitate and accelerate this trend (see paragraphs 2.11 to 2.13).

2.4 Despite the notable progress described above, there is still a tremendous contrast in how different types of companies in Chile are integrating into the digital economy and using ICT. The largest and most dynamic companies are adopting ICT more quickly and on a greater scale, and a large gap exists with respect to the microenterprises and small and medium-sized businesses (MSMBs), which are lagging considerably in the use and incorporation of the new technologies. The lower connectivity indices of this sector, which constitutes the largest part of the Chilean economy's business base,[4] are a reflection of cultural and economic barriers that hinder high rates of growth.

2.5 By 2001, 61% of Chilean companies had some form of Internet access, and 11% had developed their own websites. In the MSMB sector, the Internet is still mainly

---

[2] The most dynamic sectors of the digital economy are the nontraditional ones, such as the market for Internet access, particularly broadband, e-commerce, e-business applications, distance applications under the application service provider scheme (ASP), Internet payment methods, electronic certification, hosting services, e-learning and online advertising. All of these sectors, however, are far from maturity, which means that as a group, they represent only a small fraction of the digital economy. The most mature or 'traditional' sectors, such as fixed-line telephone communication services, the hardware industry and some sectors of the software industry, grew at a slower rate, even though they continue to represent the largest part of the so-called new economy.

[3] In the case of e-commerce, cost reductions of at least 10% have been observed for Internet transactions compared with traditional physical channels. For the e-learning model, evidence exists that operational savings above 60% have been achieved in training procedures, while savings using the ASP model have reached approximately 35%. The foregoing indicates that companies using these technologies more intensively are, in fact, creating competitive advantages in their markets.

[4] Of a total of about 580,000 existing firms in Chile, the large majority are microenterprises (82%), while small businesses represent 15% of the total. By contrast, medium-sized and large businesses are only a marginal fraction of the number of productive units in the country (2% and 1%, respectively). The composition of total sales, meanwhile, is the inverse of the business structure pyramid: while the large companies generate 72% of total sales in the economy, the microenterprises are responsible for just 4%. Even if the broader MSMB sector is considered, 99% of the total number of companies in Chile generate scarcely 29% of the country's sales of goods and services.

used for e-mail communication and searching for information (98% and 93% of connected companies, respectively). A limited number of Chilean MSMBs seem able to optimize ICT use in order to increase productivity and lower costs for their businesses.

2.6 This is due to the fact that the appropriation of technology is not an easy process, but rather a very complex one. The principal barriers that stand in the way of Chile's MSMB sector's adopting digital technologies and e-commerce include entrepreneurs' lack of knowledge about the nature, usefulness and application of new technologies and, in particular, the fear they engender with respect to critical business areas, such as privacy of information, confidentiality of communications, and security of transactions.

B. Security and trust in e-commerce

2.7 Creating an environment of security and trust is critical for increasing the use of Internet and e-commerce tools among Chilean MSMBs. However, the use of security mechanisms in Chile has progressed slowly. This is due to a number of factors, including: (i) the absence of a critical mass of electronic transactions that would generate significant demand for tools such as certification; (ii) a great lack of awareness on the part of users, particularly MSMBs, about the real risks involved in electronic transactions via insecure media, thus making it difficult to create a strong demand for digital security;[5] and (iii) until mid-2002, certification activity in Chile was carried out without legislation regarding the validity of digital signatures and electronic contracts, a factor that limited its development.

2.8 **Electronic transaction security and digital certification:** Digital certification technologies make it possible to authenticate, maintain confidentiality, ensure integrity and eliminate the possibility of refusal by any person involved in an electronic transaction, while at the same time preventing fraud at each stage of the process.

2.9 An analysis by the Center for Studies on the Digital Economy (CED) concluded that the local market is lagging in the adoption of website security standards that would make local business websites trustworthy in the eyes of users. Only 12% of Chilean websites post privacy policies and 17% post security policies. The local use of certification tools is still at a very incipient stage. While 34% of websites in the United States have electronic certification, in Chile only 2% meet this basic security standard. These deficiencies in the use of security technologies limit the

---

[5] Normally, people are familiar with the best known type of fraud the theft of credit card numbers—which is why some users avoid online purchases. However, there are many other security risks that users are not usually aware of, such as the impersonation of individuals, companies, and websites, and e-mail violation. This lack of awareness inhibits the creation of a greater demand for security tools.

possibilities of local sites for interaction with foreign sites and users, which are beginning to demand standards in this area.

2.10 With respect to the potential demand for digital certification, as of 2001, nearly 1,500 electronic certificates had been issued in Chile, mainly aimed at protecting e-mail communications (66%). The size of the market for these services was just under US$200,000, reflecting its embryonic state. By 2002, the certification market could reach US$700,000, and while the relative size of the certification market is still limited, growth rates are expected to be high over the next few years (over 70%) and the market is expected to approach US$3 million in about 2004.

2.11 **Electronic signature law and self-regulation:** Chile now has a modern Electronic Signature Law, which regulates the use of certification models and confers legal validity on electronic contracts, as well as providing government incentives for electronic invoicing. This will make it possible to lay the foundations for increasing the use of security technologies.

2.12 When transactions are carried out without the physical presence of the parties involved, the door is left open to computer crimes that threaten the concept of information as a collective juridical right. It is in this context that the law concerning electronic documents, electronic signature and certification services was enacted in March 2002 and its regulations were issued recently. These measures constitute an important contribution to Chile's digital economy, by increasing the efficiency of electronic transactions, whether they be contracts, purchases, funds transfers, etc. In addition, the law is expected to increase the transparency of bidding processes that the government carries out electronically. It will help create new markets, generate more flexible production networks among different companies and make the public and private sectors more efficient, thus achieving significant advances in productivity.

2.13 However, merely enacting the law does not mean that it will immediately be implemented in commercial processes and documents. To ensure transparency, automate some aspects of the judicial process and guarantee that the system will function well, the business sector must self-regulate the policies and standards related to privacy and security, good business practices, and integrity of e-commerce transactions.

C. Rationale for the proposed program

2.14 Based on initiatives for security and trust in e-commerce, the CCS—which is the professional association representing the largest number of Chilean businesses—has been preparing a self-regulation plan for e-commerce transactions, together with a seal of trust program and alternative conflict resolution program (ASR). In addition, it has prepared an initiative focused on providing cutting-edge electronic security solutions for businesses, through e-certchile.

2.15 **Self-regulation** is a mechanism that makes it possible to create a culture of protection and respect for the consumer, while at the same time avoiding the proliferation of local government regulations that tend to impose restrictions on businesses that—like e-business—require flexibility because they are in a constant process of technological change. One important attribute of self-regulation is its potential for avoiding the proliferation of legal initiatives that tend to overregulate matters related to information technology. It is evident that no legal regulation can evolve at the same speed as ICT, and for this reason the private sector must take the initiative in this regard.[6] In order to put this concept into practice, on the initiative of the CCS, the "Alianza por las Buenas Prácticas en Internet" [Alliance for Internet Best Practices] (ABP) was established, in which various important private-sector actors in the Internet field play a role.[7] It also has the support of important government bodies such as the Ministry of Economy, the Ministry of the General Secretariat of the Presidency, and the Ministry of Transportation and Telecommunications.

2.16 The certification initiative was developed through the creation of the first national certification authority, **e-certchile**, which was established as a joint initiative of the CCS and the Asociación Chilena de Empresas de Tecnologías de la Información [Chilean Association of Information Technology Companies] with the backing of CORFO, to provide high-quality digital certification services that are recognized and accepted both nationally and internationally. E-certchile's objective is to record and guarantee the identity of the parties who do business over the Internet, as well as the integrity of the content of their transmissions, and the acceptance of commitments made in an environment of confidentiality.

2.17 The objective of this program, which will be executed by the CCS, is to integrate the different initiatives in the field of e-commerce in order to generate trust in the new information and Internet technologies, promoting increased usage and, with that, the associated social, cultural and economic benefits. To accomplish this, however, the community must undergo long-term cultural change. This will develop—through security and respect for the privacy of personal information—the elements that are needed in electronic transactions in order to increase e-commerce in Chile.

---

[6] This model is similar to the one used by such organizations as Online Privacy Alliance and the Better Business Bureau (BBB) in the United States and in Europe by the Association of European Chambers of Commerce in partnership with the BBB and the Direct Marketing Association.

[7] In addition to the CCS, which acts as the ABP's coordinator, executing agency and executive secretary, the founding members include the Asociación de Bancos e Instituciones Financieras [Association of Banks and Financial Institutions], the Asociación Chilena de Tecnologías de la Información [Chilean Information Technologies Association], the Asociación de Proveedores de Internet [Association of Internet Providers], the Universidad de Chile, and the Colegio de Abogados de Chile [Chilean Bar Association].

2.18 The proposed program falls within a broader strategy developed by the CCS to fully support the use of ICT to make Chilean MSMBs more competitive. Among the complementary initiatives supported by the CCS, the Programa "PyME 21" (SME 21 program) stands out. This program cofinances consulting services aimed at improving business management by incorporating ICT. SME 21 diagnoses potential beneficiary companies, identifying the needs for incorporating these technologies into their procedures and helping the companies learn about the potential uses of ICT in their businesses to improve production and product quality.

2.19 The need to improve MSMB competitiveness by increasing efficiency, thus making it possible to reverse the drop in employment levels and profit margins, is an important challenge for the future development of this business sector in Chile. In this context, the use of ICT in the various production and business processes constitutes one of the elements with the greatest potential for improving the efficiency and competitiveness of the Chilean economy in the medium and long terms.

2.20 The proposed program is consistent with the objectives of the MIF's ICT cluster since the performance of SMEs will improve as will their access to markets through the increased use of ICT. In addition, it is a highly innovative program in that it seeks to create a comprehensive package of security and trust in e-commerce, the first of its kind in Latin America. For this reason, it is expected to help generate important experiences that can then be emulated and replicated in other countries of the region. Because of the aforementioned innovative aspects and its demonstration effects vis-à-vis the private sector, the proposed program will help lay the foundations for the design of future ICT-related operations.

2.21 With regard to additionality, the MIF's participation in the proposed program will make it possible: (ii) for high-level international experts and consultants with advanced knowledge of cutting-edge security solutions for e-commerce to participate in the program and provide technical support to the country; (ii) to increase the quality of technological services to be offered to MSMBs through the SICE component; (iii) to learn about security and trust in the e-commerce market from successful experiences and international best practices; and (iv) to assimilate experiences stemming from program execution and disseminate lessons learned and potential benefits to the private sector in other countries. It is believed that the CCS would not be able to achieve these results without support from the MIF.

III. PROGRAM OBJECTIVES AND COMPONENTS

3.1 The overall objective (end) of the program is to help improve the competitiveness of Chilean MSMBs. The specific objective (purpose) is to develop security services and applications and establish self-regulation mechanisms and good Internet

practices, thereby generating trust in the new information and Internet technologies, and encouraging their expanded and productive use throughout society.

3.2 This operation is structured around two main components and two supporting components: **(i) generation of confidence in the Internet environment: self-regulation–seal of trust–conflict resolution for e-commerce (ASR)**; and **(ii) comprehensive security for e-commerce (SICE).** These components complement each other inasmuch as the ASR program (component 1) will establish the comprehensive system that makes it possible to create a culture of protection, thus promoting confidence in the e-commerce market. In turn the SICE program (component 2) will provide companies with the technological tools to make commercial transactions over the internet secure. In addition, the following cross-cutting support components will be implemented: (iii) dissemination and communication; and (iv) monitoring and tracking.

1. Component 1: Generation of confidence in the Internet environment: self-regulation – seal of trust – conflict resolution for e-commerce (ASR) (MIF: US$170,000; Local: US$92,500).

3.3 This component provides for the standardization and subsequent dissemination of policies and standards related to privacy and security, good business practices, and integrity of e-commerce transactions.

3.4 The ASR component will be carried out under the auspices of the ABP through three parallel and interrelated subcomponents, whose objective is to generate trust in the Internet environment: **(i) Self-regulation (US$25,000)**, which will support the CCS in designing and establishing standards for privacy, security and good e-commerce practices. With support from international consultants, the CCS and the ABP will perform an analysis of international best practices to promote the adoption of the most secure and reliable system; **(ii) Seal of trust (US$92,500)**, which aims to set up a system of virtual seals for business websites that comply with the standards and good practices established. The CCS will enter into an agreement with an international organization whose seal and practices are already accepted and recognized by the majority of Internet users; and **(iii) Conflict resolution (US$145,000)**, which will establish a virtual conflict resolution system. This will require the development of software and the procurement of a suitable technological platform.

2. Component 2: Comprehensive security for e-commerce (SICE) (MIF: US$419,000; Local: US$506,500)

3.5 Objective of this component (SICE) is to provide cutting-edge e-business security solutions. The SICE is expected to help create an atmosphere of trust that will facilitate Internet-based transactions and business operations through the provision by e-certchile of electronic security services to companies and internationally

recognized digital certificates issued locally, which individuals and companies can use to verify their identities over the Internet. To achieve the adequate and widespread use of digital certificates in operations and transactions executed over communication networks, there should be a number of applications that provide concrete benefits to digital certificate users, particularly the MSMBs. With this in mind, the SICE component includes two subcomponents:

3.6 **(i) Development and implementation of basic digital certification services (US$562,500)**, to enable e-certchile to provide internationally recognized digital certification services on a national level that comply with Chilean legislation. However, even though e-certchile is currently the leader in digital certification, in order to fulfill its mandate, it still must comply with the requirements of the new Digital Signature Law and regulations in order to be accredited as a certification authority by the Ministry of Economy. In addition, a complete review of its initial technology strategy was carried out, with a view to reducing the costs and risks associated with developing its own digital certification software; as a result, CCS decided to procure digital signature certification services from an internationally recognized company that would also be responsible for any necessary technological updates. To carry out these activities, the following will be financed: (i) legal, technical and market analysis of digital certification; (ii) development and implementation of the International Registration Authority; (iii) preparations to make it possible to obtain the accreditation issued by the Ministry of Economy; (iv) implementation of the local Public Key Infrastructure (PKI)[8]; and (v) training for CCS and regional agency staff.

3.7 **(ii) Development of value-added services for MSMBs (US$363,000)**, to support e-certchile in developing the following value added technological services: **(a) document digitalization and custody**, to enable companies and other users to keep digital copies of their most important documents in a secure environment; **(b) electronic invoicing**, a service to enable companies to issue electronic invoices that are legally valid in Chile; **(c) electronic notary office**, to provide greater flexibility and speed for certain business procedures; and **(d) digital signature server**, to strengthen the security of the digital signatures authenticated by e-certchile. This subcomponent will primarily finance the costs of developing and procuring software and hardware to enable it to offer these services. The value-added applications and services should help improve and streamline companies' business and administrative procedures, thereby reducing costs, as well as the risks related to document handling and custody.

---

[8] This Public Key technology uses asymmetric mathematical algorithms consisting of a unique pair of keys (public and private) that work together for the signature and its verification. The private key enables the digital signature to be applied to an electronic document, while the public key enables it to be verified.

3. Component 3: Dissemination and communication (MIF: US$190,000; Local: US$50,000)

3.8 Through this component, MSMBs will receive basic information about the importance, potential and benefits derived from the digital tools to be provided through the self-regulation and digital security subprograms. In cooperation with the regional chambers of commerce, special care will be taken to promote participation by indigenous business communities as beneficiaries of the proposed program.

3.9 The activities to be carried out through this component include: (i) communications strategy and image design and development; (ii) awareness courses, seminars and workshops for companies on a national level; (iii) specialized media campaigns; and (iv) development of material for the dissemination to the MSMBs.

4. Component 4: Monitoring and tracking (MIF US$65,000; Local US$35,000)

3.10 The objective of this component is to monitor the changes in Internet best practices related to security and privacy problems, on a national and international level. The following activities will be carried out under this component: (i) quarterly survey of users that reports on Internet security and trust indicators; (ii) international benchmark studies within the framework of the World Internet Project;[9] (iii) survey and monitoring of best practices with respect to security and trust; and (iv) tracking of user behavior related to Internet security and privacy.

IV. EXECUTING AGENCY AND IMPLEMENTATION MECHANISM

4.1 The CCS will be the program executing agency. This institution has more than 1,300 voluntary members that include large, medium-sized and small businesses from the most representative sectors of the Chilean economy. The CCS has carried out a series of ICT-related projects that have had an important impact on Chile's business sectors and on society in general. These projects have been approached from different perspectives and have involved studies, information dissemination, training and education, communications, and management support for SMEs. Moreover, the projects have been made available to CCS member companies and to the general public.

4.2 For purposes of program execution, the CCS will establish a program coordinating unit (PCU) that will be located at the CED, the CCS unit specializing in ICT-related

---

[9] *World Internet Project* is an international initiative started by the Center for Communication Policy of the University of California, Los Angeles, the objective of which is to analyze and compare Internet use and the impact thereof on economic conditions and society.

research, which will carry out the planned studies and research, either directly or through external consultants. Under the CED's general coordination, the Centro de Arbitraje y Mediación [Arbitration and Mediation Center] (CAM) of the CCS will be in charge of implementing the ASR component, while e-certchile will be responsible for implementing the SICE component. To coordinate program execution, the PCU will consist of: the general coordinator, a technical-administrative coordinator, and coordinators of the ASR and SICE components. Additionally, the CSS will provide administrative and accounting support.

4.3 To protect security and trust in the process, the law requires digital certificates to be delivered by physical means initially, through which it will be possible to verify the background of the applicant. This requires the creation of a national network of registration authorities. For this purpose, e-certchile has established agreements with the principal regional chambers of commerce and industry so that they may act as a registration network for the delivery of digital certificates in different regions of the country.

4.4 It is important to note that the CCS has had successful experience with the MIF program "Expansion and Improvement of Commercial Arbitration and Mediation Services" (ATN/MT-6376-CH). To date, the CAM in Santiago has acquired vast experience in commercial arbitration and mediation management.

4.5 **Revolving fund**. Technical-cooperation resources will be disbursed through the mechanism of a revolving fund containing 10% of the total amount of the MIF contribution, as established in Bank procedures. The project resources from the MIF contribution and the local counterpart will be deposited and administered by the CCS through separate bank accounts in the name of the project. Within 60 days of the close of each six-month period, the CCS will present a semiannual report to the Bank on the status of the revolving fund under its control.

4.6 **Accounting**. The CCS will establish and will be responsible for maintaining accounting and financial systems and an internal control structure for the handling of project resources and for maintaining filing systems for supporting documents relating to expenditures of project resources, in order to be able to identify the sources and uses of program funds. The accounting system will be organized so as to provide necessary documents, facilitate verification of transactions and enable timely preparation of financial statements and reports. The CCS will also be responsible for opening separate and specific bank accounts for the administration of the MIF contribution and the local counterpart funds. Lastly, the CCS will process disbursement requests and their corresponding expense vouchers according to the Bank's disbursement rules. It will also prepare a final audited financial statement on program expenses and present it to the Bank.

4.7 **Financial audits**. During the ninety (90) days following the final project disbursement, the CCS will prepare and submit to the Bank the final financial

statements related to the Bank's contribution and to the local counterpart funds. A firm of independent auditors acceptable to the Bank will audit these financial statements pursuant to terms of reference previously agreed upon by the Bank. The cost of the audit will be financed from the MIF contribution, and the auditor selection and contracting process will be conducted according to Bank procedures (AF-200).

4.8 **Procurement.** The CCS will procure goods and services and contract the consultants necessary for the execution of the project, in accordance with the pertinent Bank and MIF procedures and policies.

4.9 **Readiness.** The CCS, with the support of the Bank's team, has prepared preliminary terms of reference for the principal consultants, as well as a three-year business plan for implementing the two main components and an execution timetable for each component's activities.

V. COST, SOURCE OF FINANCING AND COST RECOVERY

5.1 The total project cost has been estimated at US$2 million divided into: (i) US$1 million from the Bank using MIF funds [Technical Cooperation Facility I] on a nonreimbursable basis; and (ii) US$1 million in counterpart funds to be contributed by the CCS. A summary of the main project cost and financing items is presented below.

Table 1
Costs (US$)

BUDGET ITEMS	MIF	LOCAL FUND	TOTAL	%
Component 1: Generation of trust in the Internet environment (ASR)	**170,000**	**92,500**	**262,500**	**13.1**
Subcomponent 1.1: Self-regulation	17,500	7,500	25,000	1.2
Subcomponent 1.2: Seal of trust	62,500	30,000	92,500	4.6
Subcomponent 1.3: Conflict resolution	90,000	55,000	145,000	7.3
Component 2: Comprehensive e-commerce security (SICE)	**419,000**	**506,500**	**925,500**	**46.3**
Subcomponent 2.1: Digital certification	264,000	298,500	562,500	28.1
Subcomponent 2.2: Development of value-added services for MSMBs	155,000	208,000	363,000	18.2
Component 3: Communication and dissemination strategy	**140,000**	**50,000**	**190,000**	**9.5**
Component 4: Monitoring and tracking	**65,000**	**35,000**	**100,000**	**5.0**
Project administration	45,000	275,400	320,400	16.0
Evaluations and audit	65,000	0	65,000	3.3
Contingencies	96,000	40,600	136,600	6.8
TOTAL	**1,000,000**	**1,000,000**	**2,000,000**	**100.0**
%	50%	50%	100%	

5.2 **Execution and disbursement period:** The execution period will be 36 months, with a disbursement period of 42 months.

5.3 **Sustainability**: The sustainability of the services to be provided by the proposed program will depend on increased Internet use as a tool for generating and completing business transactions in Chile. For this reason, the first component is essential for guaranteeing the program's sustainability and success.

5.4 Indeed, although the ASR component, unlike the SICE component, does not include large spillovers derived from its activities, the benefits of the ASR component will be measured in terms of its success in meeting its objective of promoting Internet use in business transactions, thanks to greater trust on the part of users. In this regard, Chile's potential market is large enough to adopt the products to be offered through the program. This is because—as was mentioned in the beginning of the document—although a large number of institutions and companies have websites and use the Internet to carry out different types of business transactions, relatively few websites have adopted explicit privacy and security policies, and even fewer have electronic certification.

5.5 According to the SICE component's business plan, e-certchile may reach the operational breakeven point by 2004. After that, operating results are expected to increase gradually, so that by 2006, the program as a whole (including the ASR

component and expenses for dissemination, communication, monitoring and tracking) will become operationally sustainable. It should be noted that the surpluses generated by the SICE component services will be used to defray the operational deficit of the ASR component.[10]

5.6 Notwithstanding the foregoing, and with the aim of establishing additional self-sustainability mechanisms, a system of user charges for the ASR system will be instituted, so that users will participate in financing its operation: (i) membership fee for participants in the ABP; (ii) annual seal of trust fees; (iii) payment for audits and monitoring services carried out by external auditors; and (iv) payment for certain conflict resolution processes (mediation and arbitration).

VI. MONITORING AND EVALUATION

6.1 **Monitoring**. The CCS will prepare and submit project progress reports to the Bank's Country Office in Chile within thirty (30) days after the end of each six-month period, and a final report 30 days after the final disbursement. These reports will follow a format previously agreed upon with the Country Office and will cover the project activities and finances, as well as outcomes measured in terms of the performance indicators identified in the logical framework of the project. The Country Office will use these reports to oversee the progress of project implementation and to prepare a project completion report within three months after the final disbursement.

6.2 **Evaluation.** The Bank will hire individual consultants to carry out two project evaluations. A midterm evaluation will be carried out once 50% of the funds have been disbursed. A final evaluation will be performed three months after the end of the project. Based on the midterm evaluation, the Country Office, together with the project team, if necessary, will carry out performance evaluations to determine whether the project should be continued, suspended or cancelled. During the execution of the project, the CCS will compile the project supervision and evaluation indicators, which are presented in the logical framework (see Annex I). The Country Office and the CCS will use them to monitor the general impact and the outcomes of the program. In addition, under the "Evaluations" heading, the program includes financing, for activities related to the respective MIF cluster, such as workshops and conferences.

---

[10] The financial projections for the ASR and SICE components indicate that towards the end of the program execution period in 2006, the ASR component's operating deficit—equivalent to US$51,775—will be fully covered by the net operating surpluses of the SICE component—equivalent to some US$67,500.

VII. PROJECT RATIONALE AND RISKS

7.1 Upon termination of the program, a comprehensive and accessible mechanism should be available to guarantee security and trust in Internet-based business transactions for Chilean businesses and consumers, backed by: (i) policies and standards related to privacy, security, good business practices and integrity of transactions executed over the Internet; (ii) a system that provides for the verification of compliance with such policies and standards; (iii) a conflict resolution system for Internet transactions; and (iv) an authority that provides cutting-edge e-business security solutions.

7.2 In addition, implementation of the SICE component and of the components involving dissemination and communications, and monitoring and tracking, make it possible to achieve significant benefits in two principal areas: (a) **Market development**: The MSMBs are in the initial stage of adopting ICT. The strategy of the CCS, through e-certchile and dissemination activities, focuses on facilitating increased usage of e-business security technologies, making their benefits known, and supporting the development of business communities that use ICT to link up with each other. To promote greater use of these new electronic tools, timely support for the CCS through the program is critical; and (b) **Improvement of standards**: The new Digital Signature Law imposes high technological standards on entities registered with the Ministry of Economy. The program will provide support for e-certchile to be in a position to adapt to the more stringent requirements of the new technological standards and national and international best practices, and to implement online validation of the certificates issued.

7.3 **Risks**. The principal risks of the program are: (i) that the forecasted growth for the digital certification market may not materialize due to a lack of user interest; and (ii) that external factors, such as a change in legislation, may not permit implementation of the value-added services anticipated by the project.

7.4 During the development and structuring of the proposed program, these risk factors were taken into account and a number of mitigating actions were adopted to counteract them. These include: (i) procurement of digital certification services from an international certification company typically involves a variable cost, that is, the operating costs run parallel—in part—to the success of the service in the market, thereby enabling it to adapt more easily to possible fluctuations in the local market; in addition, the program involves intense information dissemination and education of potential users, in order to inform them of the potential benefits of adopting digital security services; and (ii) the Government of Chile has given priority to developing the information technologies market as well as online services for individual and business Internet users. Any subsequent policy developments in this field are therefore expected to favor greater adoption and use

of the Internet and of other information technology tools by Chile's various economic and social agents.

VIII. SOCIAL AND ENVIRONMENTAL FEASIBILITY

8.1 The Committee on Environment and Social Impact reviewed this operation at its meeting 35-02 held on 20 September 2002, and did not require any special evaluations or actions. The project team was advised to make an effort to ensure that indigenous companies also have access to the benefits of the program (see paragraph 3.8).

8.2 No negative environmental or social impacts are anticipated in connection with this operation. On the contrary, the program is expected to have a number of positive effects on productivity and employment levels in Chile's MSMB sector. In addition, in collaboration with the regional chambers of commerce, indigenous business communities will be encouraged to participate as program beneficiaries.

IX. SPECIAL CONTRACTUAL CLAUSES

9.1 The first disbursement of the financing will be subject to submission by the CCS of: (i) evidence of having set up the Coordinating Unit; (ii) an agreement establishing e-certchile's obligations vis-à-vis execution or component 2 of the program; and (iii) a first year execution plan, itemized by component.

X. EXCEPTIONS TO BANK POLICIES AND PROCEDURES

10.1 None.

LOGICAL FRAMEWORK

PROGRAM TO STRENGTHEN CHILEAN E-COMMERCE SECURITY AND TRUST

TC-02-05-02-4-CH

NARRATIVE SUMMARY OF OBJECTIVES	INDICATORS	MEANS OF VERIFICATION	ASSUMPTIONS
END			
Help improve the competitiveness of Chilean microenterprises and small and medium-sized businesses (MSMBs)	▪ Participation of MSMBs in the domestic economy through employment, output and sales ▪ Average MSMB productivity in terms of per-worker output	▪ Statistics related to employment, production, annual sales and productivity published by the Instituto Nacional de Estadísticas [National Statistics Institute] (INE), the Central Bank of Chile and the Centro Nacional de Productividad y Calidad [National Center for Productivity and Quality]	▪ Macroeconomic and social conditions in Chile remain stable
PURPOSE			
Develop and implement security services and applications and establish self-regulation mechanisms and good Internet practices, thereby generating trust in new information and Internet technologies, and encouraging their increased and productive usage throughout society, in particular in the MSMB sector	▪ Internet use in companies (percentage of companies with Internet connection and website) ▪ Penetration of Business-to-Business (B2B), Business-to-Consumer (B2C) and Business-to-Government (B2G) sectors (value of Internet transactions as a percentage of the total number of transactions in each of these sectors) ▪ Participation of local business websites in Internet sales ▪ Percentage of local sites using privacy and security policies and tools ▪ Number of software development companies incorporating security technology in their applications	▪ Internet use indicators prepared by the Center for Studies on the Digital Economy (CED) of the Santiago Chamber of Commerce (CCS), Undersecretariat of Telecommunications, Undersecretariat of Economy, and market research companies. ▪ Number of applications available on the market	▪ Medium- and long-term growth trends in the business sector remain stable ▪ The regulatory and legal environment continue to foster the development of electronic business media/ ▪ Market trends toward greater technological efficiency at lower unit costs remain steady

NARRATIVE SUMMARY OF OBJECTIVES	INDICATORS	MEANS OF VERIFICATION	ASSUMPTIONS
PRINCIPAL COMPONENTS			
COMPONENT 1: GENERATION OF TRUST IN THE INTERNET ENVIRONMENT			
Subcomponent 1.1: Self-regulation ▪ Design and establish standards related to privacy, security and good e-commerce practices	▪ Approval of self-regulation standards by members of the Alliance for Good Internet Practices (ABP) ▪ Number of trained officials and arbitrators (at least 10 persons)	▪ Semiannual project report ▪ ASR technical coordinator's report ▪ Publication of standards	▪ The government does not introduce new policies that might restrict private-sector e-commerce self-regulation. ▪ The participating agencies in the ABP meet ASR commitments
Subcomponent 1.2: Seal of trust ▪ The seal of trust system is installed and operational	▪ ABP approval of the accreditation and audit procedure ▪ Seal of trust software is operational ▪ ABP approval of the seal of trust ▪ Registration and participation in at least one international trust network ▪ Number of websites that are are affiliated with the seal of trust (100 websites at the end of the project) ▪ Degree to which the companies are affiliated with the seal of trust have adopted good business, privacy and security practices ▪ Change in the volume of visits and transactions experienced by the seal of trust member companies	▪ Semiannual project report ▪ ASR coordinator's report ▪ Evidence of registration in the international trust network ▪ Outcome of the monitoring of business, privacy and security practices adopted by the companies ▪ Outcome of the monitoring of the volume of visits and transactions experienced by the seal of trust member companies	▪ Local companies understand the benefits of the seal and are willing to keep up payment of fees ▪ Users value the seal positively as a guarantee of trust ▪ Technical solutions exist to prevent abuse and fraudulent use of seals of trust
Subcomponent 1.3: Conflict resolution			
▪ The conflict resolution system is installed and operational	▪ Conflict resolution management software is operational ▪ Percentage of conflicts generated under the ASR program that are channeled through the conflict resolution mechanism	▪ Semiannual project reports ▪ ASR technical coordinator's report ▪ Activity reports generated by the conflict resolution management software	▪ Companies feel that digital media is the proper channel for conflict resolution

NARRATIVE SUMMARY OF OBJECTIVES	INDICATORS	MEANS OF VERIFICATION	ASSUMPTIONS
COMPONENT 2: COMPREHENSIVE SECURITY FOR E-COMMERCE (SICE)			
Subcomponent 2.1: Digital certification ▪ E–certchile is in a position to provide companies throughout Chile with internationally recognized digital certification services that comply with Chilean legislation	▪ Accreditation of e-CertChile by the Ministry of Economy ▪ Automatic recognition by the principal browsers on the market of certificates issued by e-CertChile's international registration authority (RA) ▪ Local PKI certificates remain functional and online validation is verified ▪ 12 regional chambers of commerce authorized to provide digital certification services ▪ Number of international certificates issued (goal: year two=1,500 certificates, year three=3,000 certificates) ▪ At the end of year three, e-CertChile breaks even	▪ Evidence of accreditation by the Ministry of Economy ▪ SICE technical coordinator's reports ▪ Training registry for the 12 regional chambers of commerce ▪ Verification of e-CertChile's transactions log ▪ Verification of e-CertChile's financial statements	▪ Companies understand the benefits of certification and the use of PKI and continue to pay their fees to e-certchile
Subcomponent 2.2: Development of value-added services for MSMBs ▪ E-certchile is in a position to provide local companies with value-added technological services	▪ Availability of value-added applications: electronic invoicing, electronic notary office, digital signature server, and document digitalization and custody ▪ Number of companies using value-added applications: at least 200 using electronic invoicing, 30 using the electronic notary office, 10 using the digital signature server, and 10 using digitalization and electronic custody ▪ At least three software development companies incorporate security technology into their applications	▪ Semiannual project reports ▪ SICE technical coordinator's reports ▪ Contracts with clients for value-added services ▪ Technological partnership agreements with software development companies	▪ Local companies, particularly SMEs, understand the benefits of the services and are willing to assume the costs of such services

NARRATIVE SUMMARY OF OBJECTIVES	INDICATORS	MEANS OF VERIFICATION	ASSUMPTIONS
CROSS-CUTTING COMPONENTS			
Component 3: Communication and dissemination strategy ▪ Local companies are informed of the importance of complying with e-commerce rules of conduct and about the use of information and communication technologies, as well as seal of trust benefits and other services offered by e-CertChile	▪ At least 20 information and awareness raising events with 1,300 participating companies ▪ Two media campaigns ▪ Production of publications and graphic material	▪ Outcomes of surveys and studies carried out through component 7 (monitoring and tracking) ▪ Report of events ▪ Files on the campaigns carried out and graphic material produced	▪ No events occur that negatively affect the image of e-commerce ▪ Local companies show interest in events to be carried out
Component 4: Monitoring and tracking ▪ Surveys and studies produce the relevant data for monitoring and evaluating project performance	▪ At least 10 surveys of companies and individuals carried out quarterly ▪ Two international benchmark studies (one per year) ▪ Two studies on local best practices (one per year) ▪ At least 500 users participating voluntarily in tracking of behavior related to Internet security and privacy	▪ Outcomes of surveys and studies ▪ Progress reports from ASR and SICE subprogram coordinators	▪ Participants are found who are willing to cooperate on tracking and monitoring, for a sufficient length of time to carry out the measurements ▪ Companies are willing to provide relevant data ▪ Studies from other countries provide relevant and comparable data
ACTIVITIES			
Subcomponent 1.1: Self-regulation 1.1.1 Design of self-regulation standards 1.1.2 ASR personnel training	**BUDGET (US$)** MIF 17,500 COUNTERPART 7,500 **TOTAL 25,000**	▪ Semiannual project reports ▪ Periodic meetings of the ABP	
Subcomponent 1.2: Seals of trust 1.2.1 Design and development of seal of trust software 1.2.2 Design of the accreditation and audit procedure for applicant companies 1.2.3 Registration and participation in international trust networks 1.2.4 Survey and monitoring of best practices 1.2.5 Website maintenance and use	MIF 62,500 COUNTERPART 30,000 **TOTAL 92,500**	▪ Semiannual project reports ▪ Consultants' reports	

NARRATIVE SUMMARY OF OBJECTIVES	INDICATORS	MEANS OF VERIFICATION	ASSUMPTIONS
Subcomponent 1.3: Conflict resolution 1.3.1 Design and development of conflict resolution management software 1.3.2 Procurement of technological platform 1.3.3 Technical support for conflict resolution management software	MIF 90,000 COUNTERPART 55,000 **TOTAL 145,000**	▪ Semiannual project reports	
Subcomponent 2.1: Digital certification 2.1.1 Legal, technical and market analysis of digital certification 2.1.2 Internacional RA 2.1.2.1 Definition of requirements for International RA 2.1.2.2 Formulation of bidding documents and conditions, international call for bids, and bid evaluation 2.1.2.3 Implementation of selected solution, (initial setup) and training 2.1.2.4 Adaptation of RA standards and procedures 2.1.2.5 RA technical support 2.1.3 Accreditation—Chile's Ministry of Economy 2.1.3.1 Consulting services in preparation for accreditation 2.1.3.2 External consulting services for accreditation processes 2.1.4 Local PKI 2.1.4.1 Program for functional technical maintenance 2.1.4.2 Implementation of online certificate validation (Online Certificate Status Protocol, or OCSP): two years 2.1.5 Training for CCS personnel, regional bodies and agencies	MIF 264,000 COUNTERPART 298,500 **TOTAL 562,500**	▪ Semiannual project reports ▪ Consultants' reports	

NARRATIVE SUMMARY OF OBJECTIVES	INDICATORS		MEANS OF VERIFICATION	ASSUMPTIONS
Subcomponent 2.2: Development of value-added services for MSMBs 2.2.1 Legal, technical and market analysis of value-added services 2.2.2 Applications procurement or development 2.2.2.1 Electronic invoicing 2.2.2.2 Electronic notary office 2.2.2.3 Digital signature server 2.2.2.4 Document digitalization and custody 2.2.3 Hardware procurement 2.2.3.1 Electronic invoicing 2.2.3.2 Electronic notary office 2.2.3.3 Digital signature server 2.2.3.4 Document digitalization and custody 2.2.4 Pilot project implementation 2.2.5 Documentation of services 2.2.6 Research and development of other applications	MIF COUNTERPART **TOTAL**	155,000 208,000 **363,000**	▪ Semiannual project reports ▪ Consultants' reports	
Component 3: Communication and dissemination strategy 3.1 Image and communications strategy design and development 3.2 Awareness workshops, courses and seminars for companies 3.3 Dissemination in the media 3.4 Materials dissemination	FOMIN CONTRAPARTE **TOTAL**	140,000 50,000 **190,000**	▪ Semiannual project reports ▪ Course, seminar and workshop records ▪ Copies of advertisements published ▪ Record of materials distributed	
Component 4: Monitoring and tracking 4.1 Surveys of companies 4.2 International benchmark study 4.3 Survey and monitoring of local best practices 4.4 Tracking of user behavior related to Internet security and privacy	MIF COUNTERPART **TOTAL**	65,000 35,000 **100,000**	▪ ▪ Semiannual project reports	